

Weekly Report

June 2, 2019

1 Work

1. 图片增强任务正在尝试使用semi-supervised的setting下的结构，目前感觉加上GAN，结果会变差。
2. Adversarial Attack使用字典直接学习对抗样本，目前进攻的结果不够真实。
3. 专利修改
4. CVPR poster制作
5. 工作时长：工作日每天10个小时，周末共12个小时，共个62小时。

1.1 工作进度

Table 1: 工作进度

项目	进度	截止时间
DRGraph	正在修改代码	6.30
unpair 低光照图片增强	目前初步的实验效果不佳	7.30
Universal Flow Attack	基于字典学习Adversarial Attack	6.30

2 Paper Reading

2.1 Fast Geometrically-Perturbed Adversarial Faces

本文提出了一种基于人脸lankmark移动的方法来生成对抗样本。这种方法只需要移动少数点就可以较高的进攻效果，并且图像不会过度扭曲。

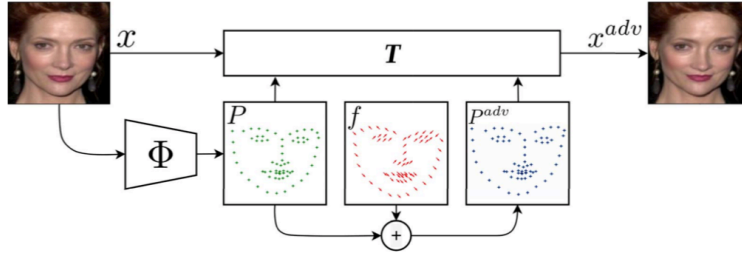


Figure 1: #1

2.2 Towards Robust Neural Networks via Random Self-ensemble

本文是提出一个防御对抗样本的方法。也就是在网络处理数据的过程中加入噪声，使得网络可以对数据有多次计算，把多次计算的结果取平均可以得到更好的效果。

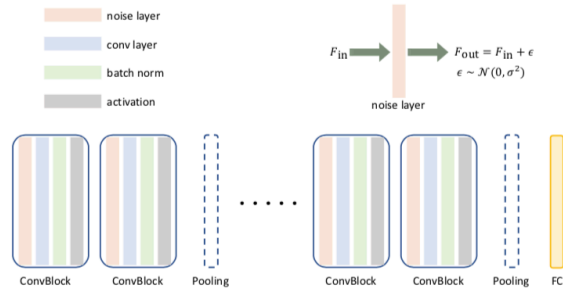


Figure 2: #2

2.3 ALIGNFLOW: LEARNING FROM MULTIPLE DOMAINS VIA NORMALIZING FLOWS

本文采用了Flow模型对CycleGAN进行改造，由于Flow模型可逆的性质，直接满足CycleGAN的循环一致性目标。作者采用Adversarial Loss和Maximum Likelihood Estimation对模型进行训练，取得了更好的效果。

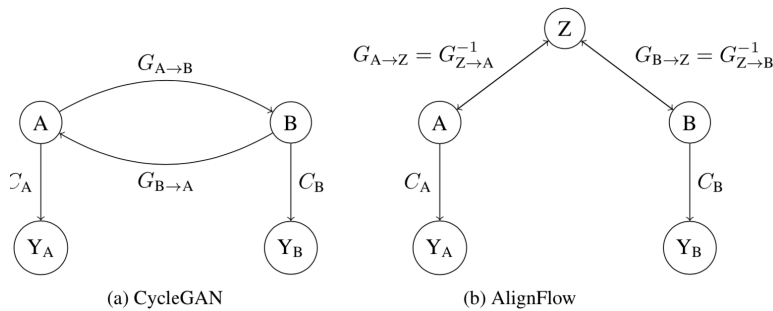


Figure 3: #3

2.4 PaperRobot: Incremental Draft Generation of Scientific Ideas

本文介绍了一种基于已有文章和知识图谱生成新文章的方法。主要内容包括1) 阅读旧论文构建知识图谱, 2) 根据用户指定的title和知识图谱找到相关的概念, 3) memory-attention networks 生成文字 (abstract和conclusion)。

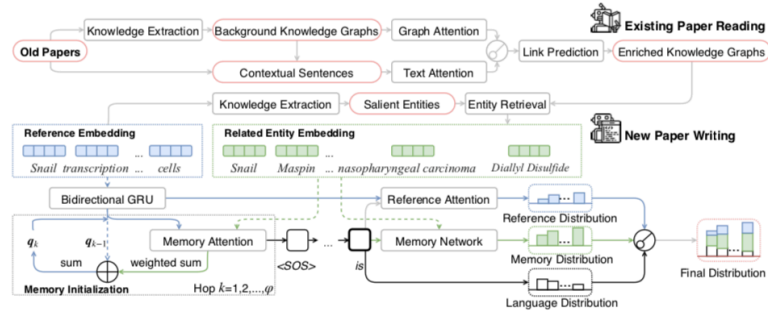


Figure 4: #4